



new era.
TECHNOLOGY



Covenant
Christian School
All knowledge through Christ

Cyber Security Preparedness *for CEN School Principals*

Presented by:
Paul Carnemolla & Solomon James

August 2023



Presenter Introduction

*Paul Carnemolla &
Solomon James*



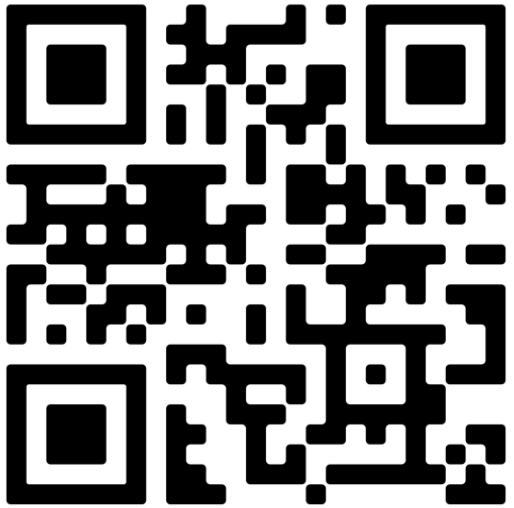
Paul Carnemolla



Solomon James



Today's resources
and further information



<https://www.neweratech.com/au/covenant-principals-conference-cybersecurity-in-schools/>



Overview

- Importance of Cyber Security in Education.
- Covenant Cyber Security Overview.
- Planning and Preparing for a Cyber Attack.
- Preparing a Cyber Security Incident Response Plan.
- Reporting to the Board.

Cyber Security Breaches

Optus – September 2022



Optus Breach Overview

EVENT
WHEN | **Optus Data Breach**
September 2022

MAGNITUDE

9.7m

**Australians
affected**

IMPACT

\$1.5m

**AUD ransom
requested**

COMPROMISED

IDs
Phone numbers
DOB
Addresses
Contact details
Passports

Optus Breach Outcome



CLASS ACTION BY LAW FIRM

- Slater and Gordon
- 100,000+ participants



REPUTATION IMPACT

- 25% Increase in Negative Media
- 13% Decrease in Positive Content



INVESTIGATIONS UNDERWAY

- Australian Federal Police
- Information Commissioner
- ACMA (Communications Watchdog)
- Denial of Human Error by Optus



MEDIA COVERAGE AFTER BREACH

- 33% Negative
- 5% Positive (Based on Meltwater)



OPTUS' RESPONSE

- Apology for Breach
- \$140 Million Allocated:
 - Customer ID Document Renewal
 - Independent Report Commissioned

Optus Breach Timeline

SEPTEMBER 22



The data breach of 11 million customer's data is discovered by Optus and Optus notified customers within 24 hours

SEPTEMBER 23



optusdata (the hacker) demands ransom of US \$1 million on the hacking forum Breached

SEPTEMBER 26



optusdata posts 10,000 customer records were breached

Home Affairs Minister Clare O'Neil blames Optus for the attack

Slater & Gordon announce its class action investigation

SEPTEMBER 27



Those affected by the breach report being extorted for their data

optusdata deletes their earlier posts and issues an apology to victims of the breach and Optus

SEPTEMBER 28



Maurice Blackburn announce its class action investigation

Cyber Security Breaches

Newcastle Grammar School – November 2020



Newcastle Grammar School

Overview

EVENT | **Newcastle Grammar School Ransomware Attack**
WHEN | **November 2020**

MAGNITUDE

90

**Students and
Staff**

affected
despite conducting a cyber
assessment 3 months prior

IMPACT

\$1m

**ransom
requested**

in Crypto Currency

COMPROMISED

IT System

Systems encrypted
lost access to core
functions (email,
phones, physical
security)

Newcastle Grammar School

Immediate Impacts



BRAND AND REPUTATION

- Became Headline News
- Challenging Communication
- Media Engagement



STAFF AND STUDENT MORALE

- Students Couldn't Attend
- Staff Workload Increased
- Exam & Report Rewrite



DATA LOSS

- Sensitive Information Lost
 - Staff Financial Records
 - Photographs
- Parent Contact Hindered



VULNERABILITIES EXPOSED

- Risk Management Flaws
- Costly Recovery & Rebuilding

Newcastle Grammar School

Outcome

“Every resource was put towards rebuilding our system as quickly as we possibly could and minimising the impact.”

~ Erica Thomas, School Principal

WHAT HAPPENED

- Malicious email opened by staff (human error)
- System protection failed

OUTCOME

- Systems restored in 5 weeks
- 1M+ files checked
- Lost: Files over 2+ months (reports, exams)

Importance of Cyber Security *in educational institutions*



Importance of Cyber Security in educational institutions

1

Protect Sensitive Data

2

Preserving Academic Integrity

3

Safeguarding Intellectual Property

4

Maintaining Operational Continuity

5

Protecting Financial Resources

6

Fostering Trust and Reputation

7

Promoting Digital Citizenship & Online Safety

8

Compliance with Regulations

9

Mitigating Cyber Threats and Attacks

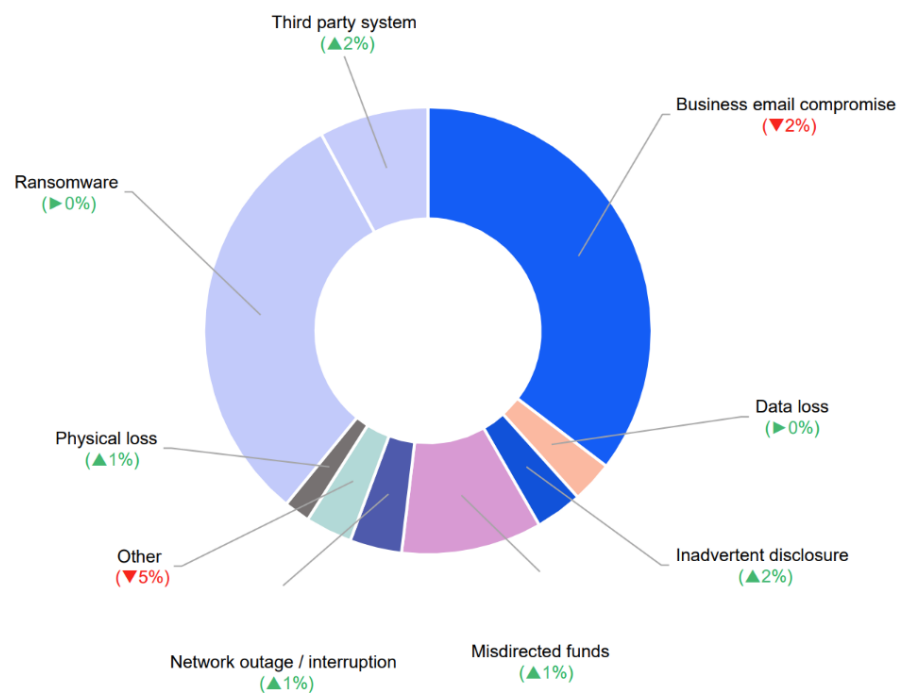
10

Preparing Students for the Future

Education sector graphic

From Clyde and Co Attack Webinar 202307.19

Incident trends in the past 12 months*



Incidents by sector

Sector	% of breaches
Healthcare	15% (▲3%)
Professional Services	13% (▼8%)
Financial Services / Institutions	12% (▼2%)
Construction	8% (▲4%)
Retail / Hospitality	8% (▼3%)
Technology	7% (▲2%)
Real Estate	6% (▲1%)
Education	5% (▲2%)
Non-profit	5% (►0%)
Transportation / Logistics	5% (▲3%)
Manufacturing	5% (▲1%)
Entertainment / Recreation / Media	5% (▲1%)
Public Entity	3% (▼2%)
Charity	2% (▼1%)
Utilities	1% (►0%)

Project Timeline

The Covenant Story



REMEDIATION

INCEPTION

BASELINE

2021 • Term 3

Pre-ICT Leadership - New Era

On-premise services:

- Active Directory
- Attache (Finance)
- FileShare
- WebHelpdesk
- CounselPro

Cloudwork for MFA/SSO

Microsoft 365 A5 Suite

Hybrid Exchange in Cloud and Azure

2021 • Term 4

Penetration Test

- Internal
- External
- Wi-Fi

Disaster Recovery Planning

2021-2022 School Holidays

1st Internal Pen. Remediation

2021 • Term 3

Implementation of Intune / Endpoint Manager

Upgrade Endpoint Security

2022 • Term 4

Jamf Pro Security Audit + Jamf Connect Config

Windows 11 Configuration and AutoPilot Setup

2022-2023 School Holidays

2nd Pen. Remediation

2023 • Term 1

Secure-ISS SIEM Implementation

Security Uplift Project (x2)

2023 • Term 2

Security Awareness platform – Knowbe4

Microsoft 365 Security Audit

2023 • Term 2 (in progress)

Microsoft 365 Security Remediation

2023 • Term 3 (in progress)

Incident Response Plan – Project

Web Application Firewall

2023 • Term 4

Definitiv Cloud payroll solution

Cyber Security framework

Cyber Security Risk Assessment

2024 • Term 1

Secondary Laptop Program

Penetration Testing

Enhancing Cyber Security Through Penetration Testing

- School underwent a comprehensive Penetration Testing in Term 4 2021, covering:

- Internal Penetration tests
- External Penetration tests
- Wi-Fi Penetration tests

Finding ID	Risk	Title	Remediation Timeframe	Status
INPT-1	Extreme	Account and privilege management is not adequate.	3-6 Months	Open
INPT-2	Extreme	Password hygiene is not adequate.	1-2 Months	Open
ENPT-1	High	Multi-factor authentication is not required for external access to Virtual Private Network.	1-2 Months	Open
ENPT-2	High	Users are susceptible to email-based phishing attacks.	Ongoing	Open
ENPT-3	High	Website is vulnerable to web cache poisoning.	N/A	Closed
INPT-3	High	Systems are vulnerable to null session attack.	1 Month	Open
INPT-4	High	Students have local administrative privileges and wide-reaching network access on	Covenant to confirm	Open
INPT-5	High	Domain is susceptible to Kerberoasting attacks.	1-2 Months	Open
WNPT-1	High	Wireless LAN is not logically segmented from wired LAN.	3 Months	Open
WNPT-2	High	No Wireless Intrusion Prevention System (WIPS) implemented.	1 Month	Open
ENPT-4	Moderate	DNS server vulnerable to zone transfer.	N/A	Closed
ENPT-5	Moderate	Issues with certificates used to validate host identity.	3 Months	Open
ENPT-6	Moderate	DMARC has not been implemented.	1 Month	Open
ENPT-7	Moderate	DKIM has not been implemented on primary mail domain.	1 Month	Open
INPT-6	Moderate	Credentials are cached on workstations that are constantly connected to Domain Control	1-2 Months	Open
INPT-7	Moderate	KRBTGT account password has not been changed for an extensive period of time.	2 Weeks	Open
INPT-8	Moderate	Directory Replication allowed to hosts other than Domain Controllers.	1-2 Months	Open
INPT-9	Moderate	Domain Administrators are not restricted to Domain Controllers.	2 Weeks	Open
INPT-10	Moderate	Administrators are assigned debug privileges.	2 Weeks	Open
INPT-11	Moderate	VMware vCenter missing critical security patches.	2 Weeks	Open
INPT-12	Moderate	Issues with certificates used to validate host identity.	1-2 Months	Open
INPT-13	Moderate	802.1X authentication not implemented on wired network.	6-12 Months	Open

Microsoft Security Uplift

Security features and enablers within the suite of Microsoft products in use:

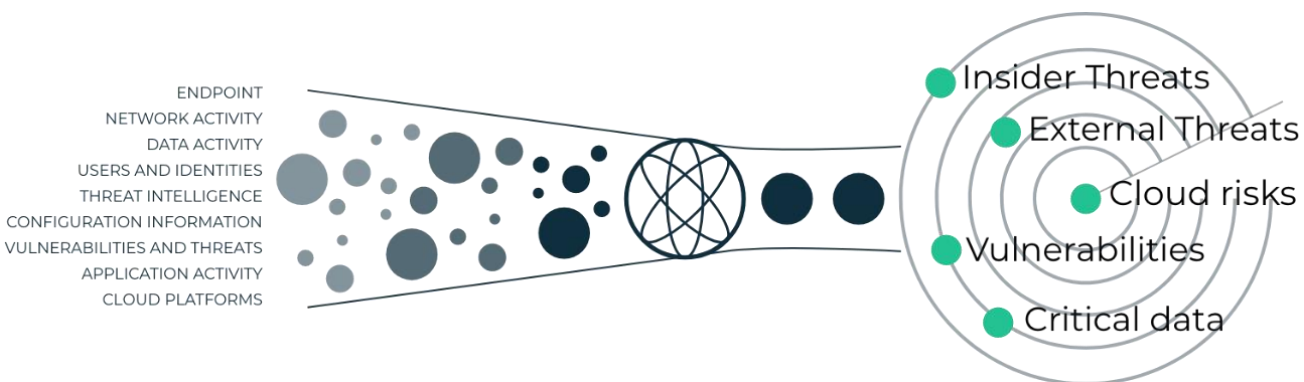
- Microsoft Endpoint Manager
- Microsoft Security Score
- Defender for Endpoint Plan 2 and Office 365 Plan 2
- Conditional Access
- Data Loss Prevention
- Compliance Program for Microsoft Cloud

[Microsoft License Feature Comparison](#)

Security Information and Event Management

Secure-ISS - <https://secure-iss.com/>

- Correlates events from all available log sources in real-time ensure threat alerts are prioritised
- 24/7 SOC (Security Operation Centre) escalate and contain identified threats
- Minimal resources required from the TechServe team



Security Event Monitoring	Secure ISS	School Resource
Deployment of virtual appliance(s) to collect and store security logs	✓	
Integration into IBM QRadar Management Console (SIEM)	✓	
Tuning	✓	✓
Monitoring & Detection (24x7)	✓	
Security Analyst - Reporting and Notification Period (8x5)	✓	
Threat Intelligence (IBM X-Force + collection/sharing of school threats)	✓	
Cloud Security Monitoring	✓	
Incident Management (Triage, Investigate, Analyse)	✓	
Security Operations Centre Touchpoints:	✓	
Live Updates of Security Incidents	✓	
Monthly Security Operation & Governance Reporting	✓	
Incident Response (Disrupt & Contain)	✓	✓
Incident Remediation	✓	✓

Security Event Monitoring is priced at **\$1 per month, per enrolled student** (based on the above scope of work / service)

Secondary Laptop Program

- Board endorsed decision to move to school managed Windows devices for secondary students
- Web filtering and content control
- Enhanced security controls
- Centralised monitoring and management
- Data protection and controlled software deployment
- Swift remediation of any vulnerability or software threats
- Conditional Access management

	4-year rollout					
	7	8	9	10	11	12
2024	x		x			
2025	x	x	x	x		
2026	x	x	x	x	x	
2027	x	x	x	x	x	x
2028	x	x	x	x	x	x
2029	x	x	x	x	x	x



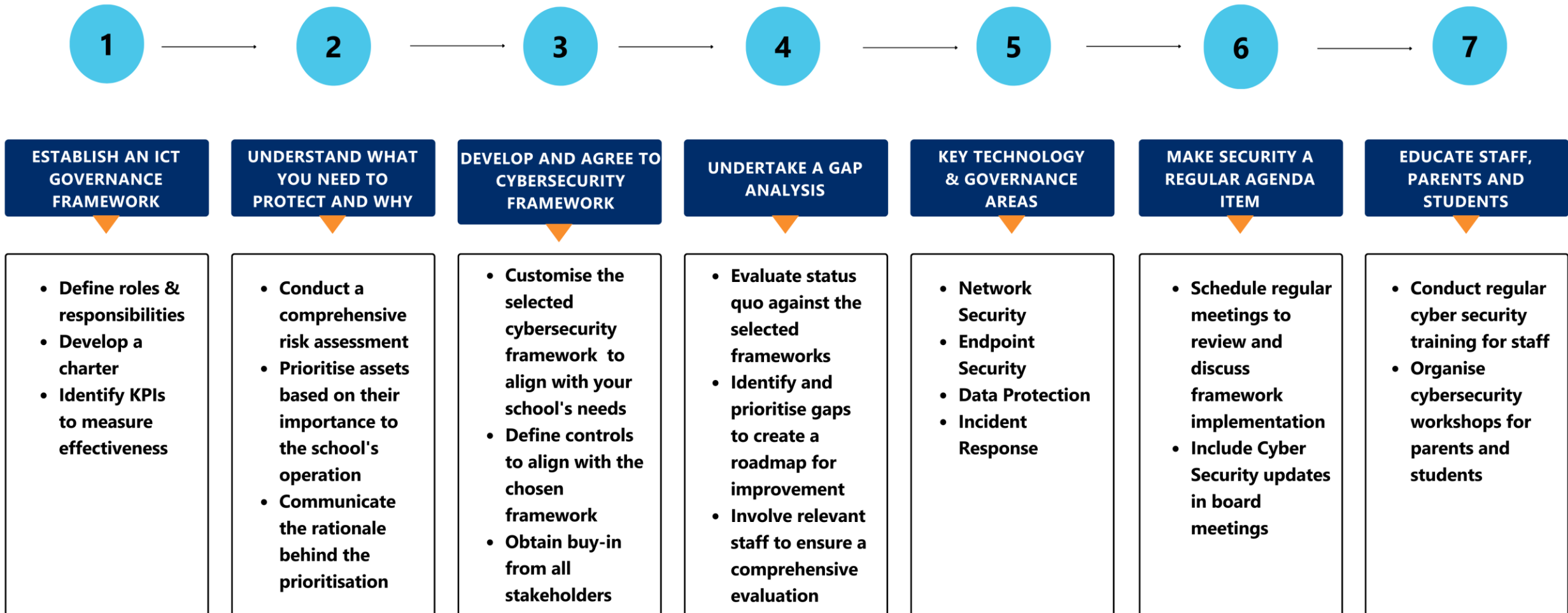
Other Key Projects

- KnowBe4 Security Awareness Training and regular Phishing campaigns
- Data Classification
- Security Improvements:
 - Enhanced network segregation
 - 802.1x network authentication for wired network
- Security Questionnaire for Third-Party Vendors
- Cyber Security Incidence Response Plan

Planning and preparing *for a cyber-attack*



Planning and preparing for a Cyber-Attack



1 – Establish an ICT Governance Framework

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

The key tasks to establishing an ICT Governance Framework with an IT Steering Committee include:



2 – What to Protect and Why?

To effectively protect your school's assets, it is crucial to understand what needs to be protected and why.

- 1 GOVERNANCE
- 2 **PROTECT**
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



What is Data and Application Mapping?

- Identify data-app relationships
- Understand data flow, access, manipulation
- School gains insights into:
 - IT data flow
 - App interaction
 - Data protection
 - Ingress/egress points to network
 - Security weaknesses

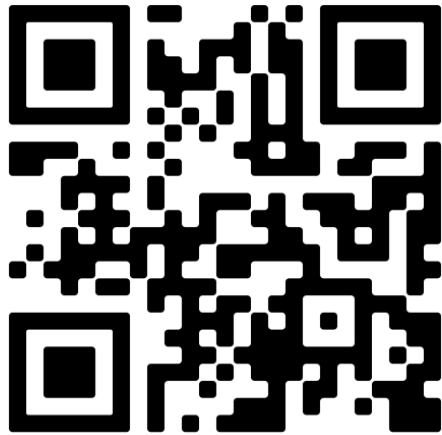
Cyber Risk Assessment

Data Map and Sensitivity Rating

- Data Sensitivity
 - Public
 - Personal
 - Sensitive
- Visual representation of risk in each system.
- Can be reviewed internally or by software provider
- Data classification categories:
 - Student and Parent Data
 - Staff Data
 - Finance
 - HR and Payroll
 - Marketing
 - Governance, Risk and Compliance
 - IT Data

Data Categories	Data Items	Sensitivity Label Impact to school if information is included in a data breach High = 5, Low = 1
Cloud or On Premise		
MFA Enabled		
Student and Parent Data	Student - Name	3
	Student - Address	4
	Student - Photos	4
	Student - DOB	4
	Student - Medical records	5
	Student - Academic Records	4
	Student - School email address	3
	Student - Mobile phone number	3
	Student - Counselling notes	5
	Student - discipline notes	5
	Student - welfare notes	5
	Parent - Name	3
	Parent - Address	4
	Parent - Phone number	3
	Parent - email address	3
	Parent - Bank account details	5
	Parent - Credit card details	5
Staff data	Staff - Name	3
	Staff - Address	4
	Staff - DOB	4
	Staff - Personal phone numbers	4
	Staff - Photos	4
	Staff - Personal email address	4
	Staff - License or other	5

Data Classification Activity



Or go to this link and click
"View Data Classification Exercise":

<https://www.neweratech.com/au/covenant-principals-conference-cybersecurity-in-schools/>

- 1 GOVERNANCE
- 2 **PROTECT**
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Data Categories	Data Items	Sensitivity Label* High = 5, Low = 1	Student Information System	HR System	Payroll System
Student and Parent Data	Student - Name	3			
	Student - Address	4			
	Student - Photos	4			
	Student - DOB	4			
	Student - Medical records	5			
	Student - Academic Records	4			
	Parent - Name	3			
	Parent - Address	4			
	Parent - Phone number	3			
	Parent - email address	3			
Staff data	Parent - Bank account details	5			
	Parent - Credit card details	5			
	Staff - Name	3			
	Staff - Address	4			
	Staff - DOB	4			
	Staff - Personal phone numbers	4			
	Staff - Photos	4			
Finance	Staff - Personal email addresses	4			
	Staff - License or other identity documents	5			
	Invoice Ledger Data	4			
	Historic Invoicing Data	4			
	Bank Details	5			
	Tax Return Data	5			
HR and Payroll	Vendor/Supplier/Contractor Contact and Bank Details for payment	3			
	Staff ID (DOB, Addresses, Copies of Identity Documents)	5			
	Salary & Payroll Data	5			
	Staff Tax File Numbers	5			
Marketing	Employee Contracts	4			
	Police Checks	5			
Governance, Risk and Compliance	Website Data	2			
	Marketing Campaign Data	2			
	Board Papers & Minutes	3			
	Breach Reports	5			
IT Data	Regulatory Reports	3			
	Risk Register Data	2			
	Incident Register Data	4			
	Infrastructure map	5			
	IT passwords	5			
	Asset Lists	5			
	Data Maps	5			

* Sensitivity Label: Impact to school if information is included in a data breach

Cyber Risk Assessment

Cyber Security Questionnaire for Vendors

Gauge how the vendors treat your data and what security practises they employ:

- Data protection
- Security and integrity
- Backups and recovery
- Compliance and certifications
- Risk management

Easy to access online questionnaire using Microsoft Forms



Or go to this link and click
"Questions to ask Third-Party Vendors":

General Security

4. What security measures do you have in place to protect against common threats like malware, DDoS attacks, and data breaches?

Enter your answer

5. Do you conduct regular security audits or penetration tests to identify vulnerabilities?

Enter your answer

6. Are your systems and applications regularly patched and updated to address known security vulnerabilities?

Enter your answer

3 – Develop and Agree to a Cyber Security Framework

Cyber Security Frameworks

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

**Essential 8
Maturity Model
Australian Cyber Security
Centre (ACSC)**

**Centre for Internet Security
(CIS) Controls**

**National Institute of
Standards and Technology
(NIST) Cyber Security
Framework**

Essential 8 (Maturity Model)

Strategies



Application control

To control the execution of unauthorised applications / software



Patching applications

To remediate known security vulnerabilities



Configure Microsoft Macro Settings

To block untrusted macros and only allow checked macros from trusted locations



User application hardening

Configure web browsers to block and disable potential malware



Restrict Admin privileges

To limit powerful access to important business information and systems



Patch Operating Systems

To remediate known security vulnerabilities



Multi-Factor Authentication

To protect against unauthorised access



Daily Backups

To maintain the availability of critical business data

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

- 1 **E8**
- 2 CIS
- 3 NIST

Essential 8 (Maturity Model)

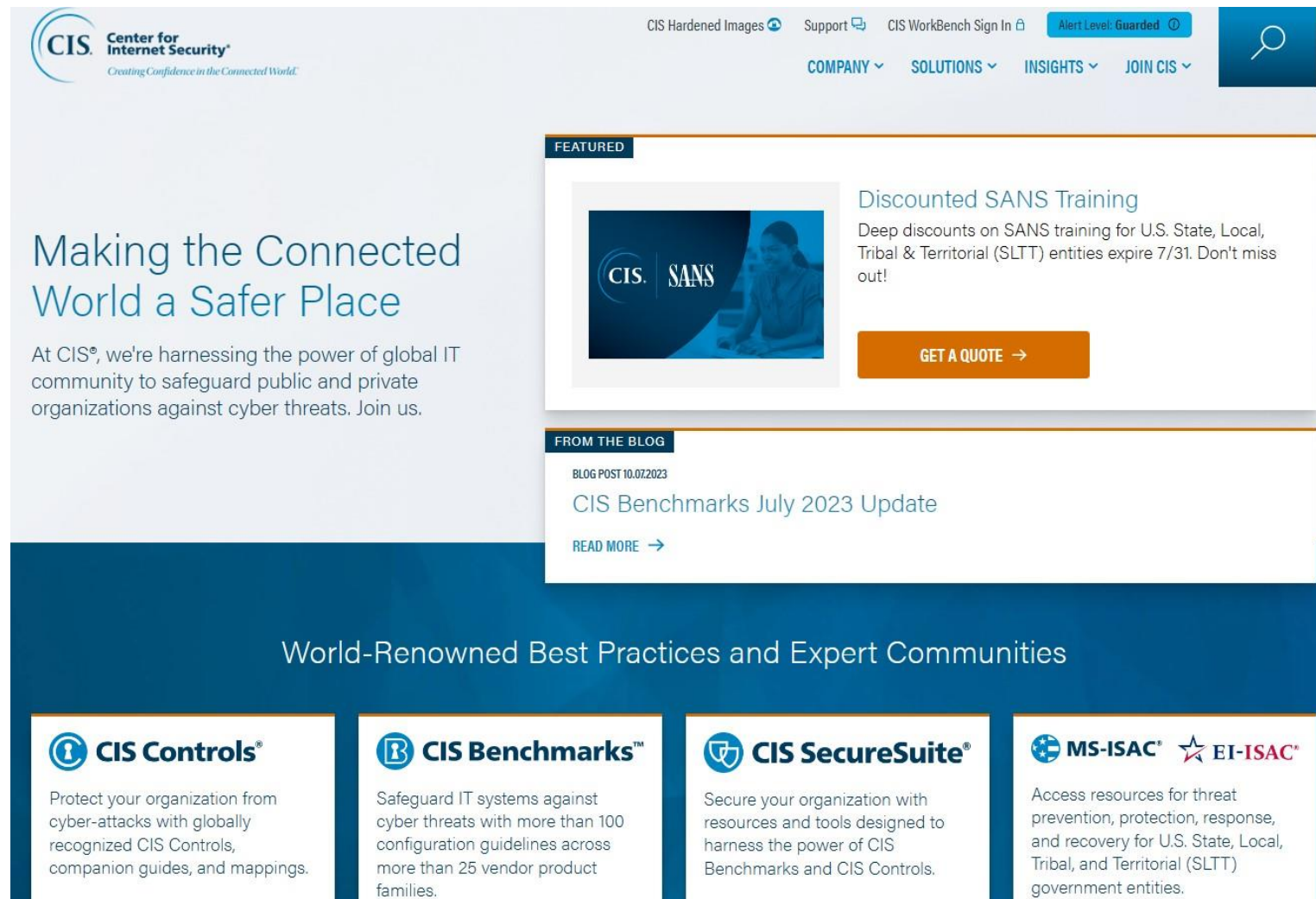
Maturity Levels



- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

- 1 **E8**
- 2 CIS
- 3 NIST

Centre for Internet Security (CIS)



The screenshot shows the CIS website homepage. At the top, the CIS logo is on the left, and navigation links for 'CIS Hardened Images', 'Support', 'CIS WorkBench Sign In', and 'Alert Level: Guarded' are on the right. Below the navigation, there are links for 'COMPANY', 'SOLUTIONS', 'INSIGHTS', and 'JOIN CIS'. The main content area features a large heading 'Making the Connected World a Safer Place' with a subtext about harnessing global IT community power. To the right, there's a 'FEATURED' section with a 'Discounted SANS Training' announcement and a 'GET A QUOTE' button. Below that, a 'FROM THE BLOG' section highlights a 'CIS Benchmarks July 2023 Update'. The footer section, titled 'World-Renowned Best Practices and Expert Communities', lists four key offerings: CIS Controls, CIS Benchmarks, CIS SecureSuite, and MS-ISAC/EI-ISAC resources.

CIS Center for Internet Security®
Creating Confidence in the Connected World®

CIS Hardened Images Support CIS WorkBench Sign In Alert Level: Guarded

COMPANY SOLUTIONS INSIGHTS JOIN CIS

Making the Connected World a Safer Place

At CIS®, we're harnessing the power of global IT community to safeguard public and private organizations against cyber threats. Join us.

FEATURED

Discounted SANS Training

Deep discounts on SANS training for U.S. State, Local, Tribal & Territorial (SLTT) entities expire 7/31. Don't miss out!

GET A QUOTE →

FROM THE BLOG

BLOG POST 10.07.2023

CIS Benchmarks July 2023 Update

READ MORE →

World-Renowned Best Practices and Expert Communities

CIS Controls®

Protect your organization from cyber-attacks with globally recognized CIS Controls, companion guides, and mappings.

CIS Benchmarks™

Safeguard IT systems against cyber threats with more than 100 configuration guidelines across more than 25 vendor product families.

CIS SecureSuite®

Secure your organization with resources and tools designed to harness the power of CIS Benchmarks and CIS Controls.

MS-ISAC® **EI-ISAC®**

Access resources for threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

- 1 GOVERNANCE
 - 2 PROTECT
 - 3 **FRAMEWORK**
 - 4 GAP ANALYSIS
 - 5 KEY TECH
 - 6 AGENDA ITEM
 - 7 EDUCATE
-
- 1 E8
 - 2 **CIS**
 - 3 NIST



CIS Controls

18 Controls

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

- 1 E8
- 2 **CIS**
- 3 NIST

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7	CONTROL 03 Data Protection 14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12	CONTROL 05 Account Management 6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

THREE LEVELS OF MATURITY

Safeguards – specific and unique actions



CIS Control - 3

Data Protection

Control	CIS Safeguard	Asset Type	Secure Function	Data Protection	IG1	IG2	IG3
3	3.1	Data	Identify	Establish and Maintain a Data Management Process	X	X	X
	3.2	Data	Identify	Establish and Maintain a Data Inventory	X	X	X
	3.3	Data	Protect	Configure Data Access Control Lists	X	X	X
	3.4	Data	Protect	Enforce Data Retention	X	X	X
	3.5	Data	Protect	Securely Dispose of Data	X	X	X
	3.6	Devices	Protect	Encrypt Data on End-User Devices	X	X	X
	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		X	X
	3.8	Data	Identify	Document Data Flows		X	X
	3.9	Data	Protect	Encrypt Data on Removable Media		X	X
	3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X
	3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X
	3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X
	3.13	Data	Protect	Deploy a Data Loss Prevention Solution			X
	3.14	Data	Detect	Log Sensitive Data Access			X

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

- 1 E8
- 2 **CIS**
- 3 NIST

CIS Benchmarks

SECURE CONFIGURATIONS

Enhance security and reduce risk by modifying system default settings.

Cloud systems such as Microsoft and Google systems prioritise functionality and collaboration over security by default.

CIS Benchmarks are leading industry practices for secure IT system configuration.



Home > CIS Benchmarks

CIS Benchmarks List

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

[DOWNLOAD BENCHMARKS](#) →

Are you new to the CIS Benchmarks? [Learn More](#)

[CIS Hardened Images](#) [Support](#) [CIS WorkBench Sign In](#) [Alert Level: Guarded](#)

[COMPANY](#) [SOLUTIONS](#) [INSIGHTS](#) [JOIN CIS](#)



Find the CIS Benchmark you're looking for



STEP 1

Select your technology.

Choose from operating systems, cloud providers, network devices, and more.

1 2 3 4

[CLOUD PROVIDERS](#)

[DESKTOP SOFTWARE](#)

[DEVSECOPS TOOLS](#)

[MOBILE DEVICES](#)

[MULTI FUNCTION PRINT DEVICES](#)

[NETWORK DEVICES](#)

[OPERATING SYSTEMS](#)

[SERVER SOFTWARE](#)

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

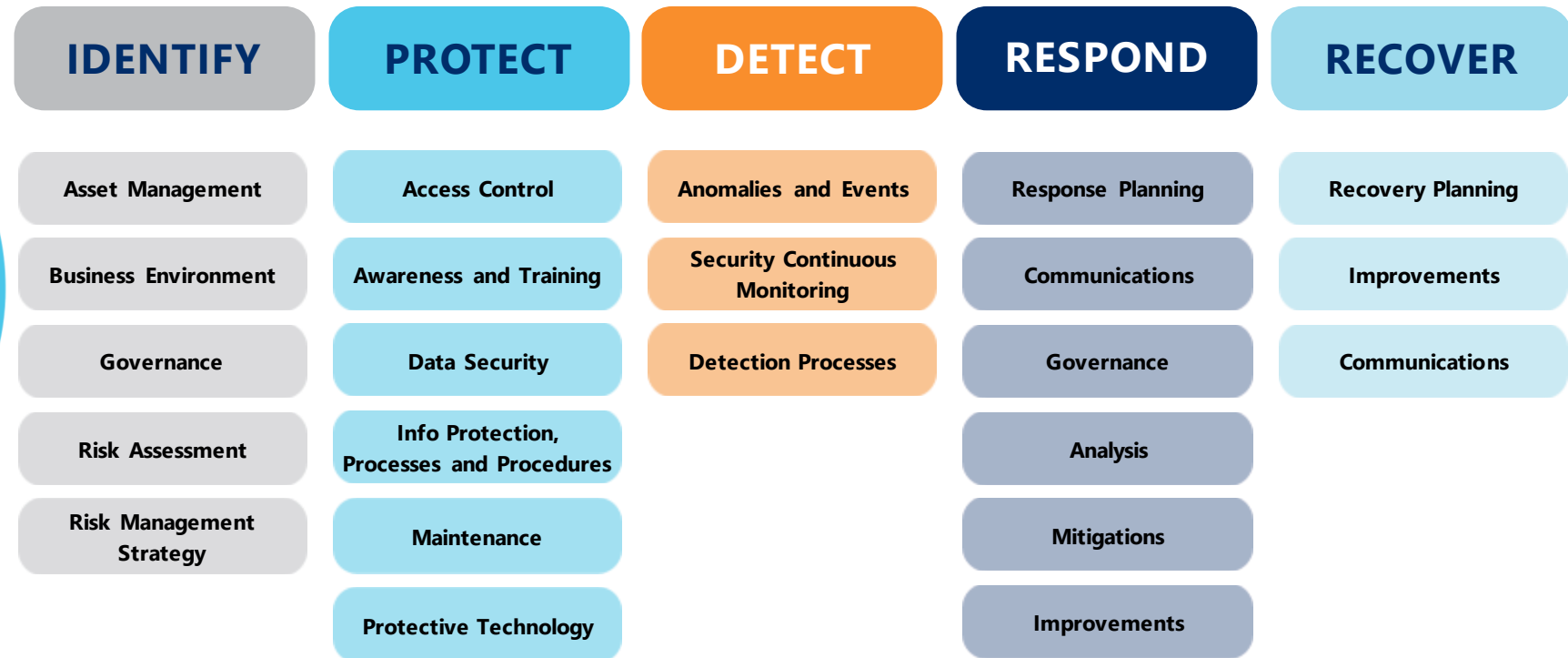
- 1 E8
- 2 **CIS**
- 3 NIST

CIS Benchmarks

Sample – iPadOS

• Restrictions	 92
○ Functionality	 93
○ (L2) Ensure "Allow screenshots and screen recording" is set to "Disabled" (Manual)	 94
○ (L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled" (Automated)	 96
○ (L1) Ensure "Allow Siri while device is locked" is set to "Disabled" (Automated)	 98
○ (L1) Ensure "Allow iCloud backup" is set to "Disabled" (Automated)	 100
○ (L1) Ensure "Allow iCloud documents & data" is set to "Disabled" (Automated)	 102
○ (L1) Review "Allow iCloud Keychain" settings (Automated)	 104
○ (L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled" (Automated)	 107
○ (L2) Ensure "Allow USB drive access in Files app" is set to "Disabled" (Automated)	 109
○ (L2) Ensure "Allow network drive access in Files app" is set to "Disabled" (Automated)	 111
○ (L1) Ensure "Force encrypted backups" is set to "Enabled" (Automated)	 113
○ (L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled" (Manual)	 115
○ (L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled" (Automated)	 117
○ (L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled" (Automated)	 119
○ (L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled" (Manual)	 121

NIST Cybersecurity Framework



- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

- 1 E8
- 2 CIS
- 3 **NIST**

- Made up of 5 core functions.
- Each function is defined.
- Within each function is a set of assessable areas

Steps to implement a Cyber Security Framework

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

Identify security Influences

- Business Objectives
- Risk Management Framework
- Government Requirements
- Other

Confirm Framework

E.g. NIST

- Identify
- Protect
- Detect
- Respond
- Recover



Identify Current State

- Scorecard
- Risk Assessment
- Gap analysis

Define Target Security Levels and Scorecard

Develop Uplift Roadmap

Progress Reports, Security Updates reported into ICT Steering Committee, School Executive and Board.

Implementing Policies – SANS and NIST

Security Policy Templates

Home > Security Policy Project

Security Policy Templates

In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted here a set of security policy templates for your use. To contribute your expertise to this project, or to report any issues you find with these free templates, please submit via the button below. Membership to the SANS.org Community grants you access to thousands of free content-rich resources like these templates. **Templates updated November, 2022!**

[Join the Community](#) [Submit Contribution](#)

Filters:

Categories

- ☐ Application Security
- ☐ General
- ☐ Server Security
- ☐ Network Security
- ☐ Incident Handling
- ☐ Retired

Acceptable Encryption Policy

Acceptable Use Policy

Acceptable Encryption Policy	+
Acceptable Use Policy	+
Acquisition Assessment Policy	+
Analog/ISDN Line Security Policy	+
Anti-Virus Guidelines	+
Automatically Forwarded Email Policy	+
Bluetooth Baseline Requirements Policy	+
Communications Equipment Policy	+
Cyber Security Incident Communication Log	+
Cyber Security Incident Form Checklist	+
Cyber Security Incident Initial System Triage	+
Cyber Security Incident Recovery	+
Data Breach Response Policy	+
Database Credentials Policy	+
Dial In Access Policy	+
Digital Signature Acceptance Policy	+
Disaster Recovery Plan Policy	+

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

4 – Undertake a Gap Analysis

to assess the Cybersecurity posture of the School

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 **GAP ANALYSIS**
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

GAP ANALYSIS STEPS

- 1 **Identify Framework Core Functions**
- 2 **Define Desired State**
- 3 **Assess Current State**
- 4 **Identify Gaps**
- 5 **Prioritise Gaps**
- 6 **Develop & Implement Plans**
- 7 **Monitor, Track, Review Progress**

5 – Key Technology Areas for a Cyber-Attack preparations

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 **KEY TECH**
- 6 AGENDA ITEM
- 7 EDUCATE

1

Network Defense

Firewalls, Endpoint Security

2

Network segregation

3

OS + App Software Maintenance

Patch OS & apps regularly

4

Access Control

Minimise admin privileges

5

Secure Authentication

Strong Passwords,
Multi-factor Authentication

6

Continuous Assessment

Vulnerability Tests,
Penetration TESS

7

Threat Protection

Intrusion Detection,
Suspicion Monitoring

8

Centralised Monitoring & Alerts

5 – Key Technology Areas for a Cyber-Attack preparations

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



6 – Make Security a Regular Agenda Item

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Establish ICT Steering Committee



Make Cyber Security an agenda item in ICT Steering Committee and Board Updates



Discuss identified gaps and risks (be transparent)



IT provides updates on framework implementation



Discuss emerging threats



Seek expert guidance and support, if required

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 **EDUCATE**



Regular Training Sessions

- Staff
- Parents
- Students



Audience-Centric Approach

- Relevant Content for Roles



Focus Areas

- Password Security
- Phishing Awareness
- Social Engineering
- Safe Browsing
- Data Privacy
- Responsible Social Media Use



Promote Reporting & Communication



Acceptable Use of Resources

- School Equipment & Systems

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Consistent Reinforcement

- Regular Cybersecurity Practice



Audience-Centric Approach

- Relevant Content for Roles



Addressing Cyberbullying



Teaching Digital Citizenship



Managing Screen Time

- Implementing Parental Controls



<https://www.esafety.gov.au/parents/issues-and-advice>

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

To educate staff, parents and students on Cybersecurity effectively:



Audience Relevance

- Tailored Content
- Role-Specific Information



Consistent Reinforcement

- Regular Cybersecurity Practice



<https://www.covenant.nsw.edu.au/parent-resources/technology-support/technology-advice-for-parents>

7 – Educate Staff, Parents, and Students

KnowBe4

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 **EDUCATE**



Phishing Defense

- Regular Tests & Training
- Guard Against Social Engineering



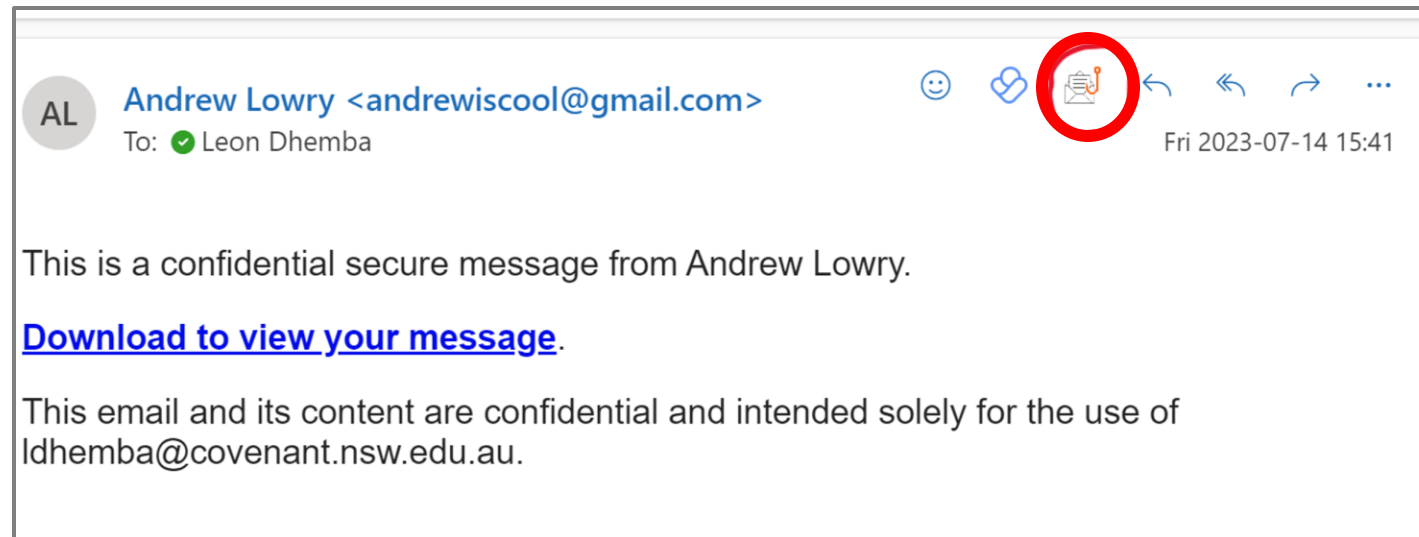
Phishing Reporting

- Simplified Alert Process
- Webmail & Email Client Button



Assessment Measures

- Baseline & Follow-up Checks



Preparing a Cyber Security *incident response plan*



Incident Management



INCIDENT



PROCESS



DETECTION



ANALYSIS

- A cyber incident is any attempted or actual unauthorised access.



**INITIAL
SUPPORT**



RESTORE



REPORTING

- The goal of incident response is to detect and halt attacks.

Risk Management Terms

ASSET

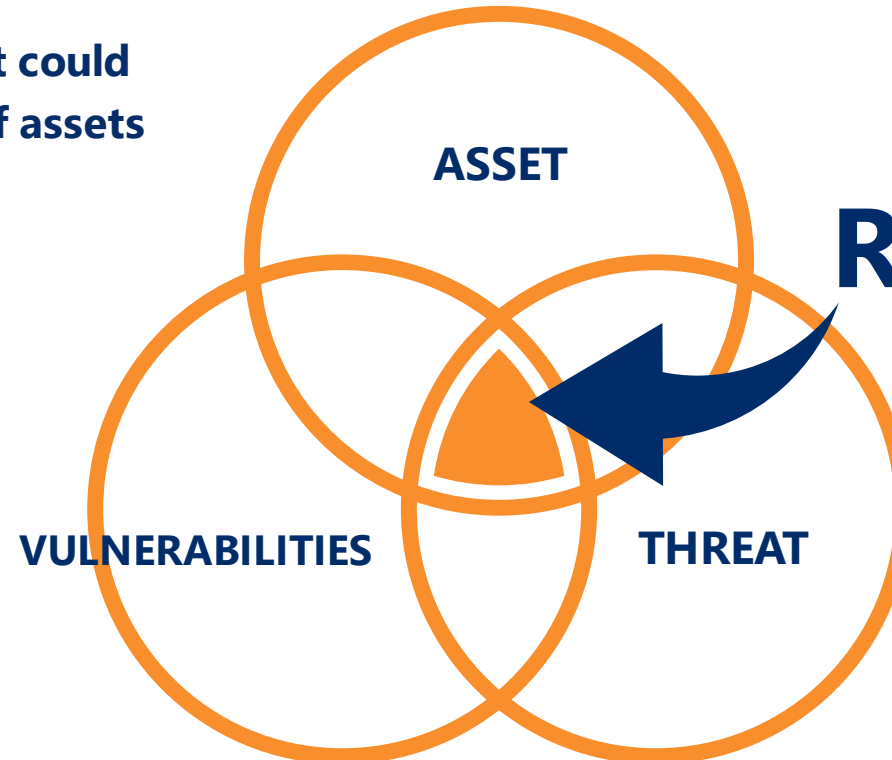
Anything of value

VULNERABILITIES

Weakness or flaw that
could be exploited

THREAT

Something that could
lead to a loss of assets



RISK

Potential for loss/damage
of an asset when a threat
exploits a vulnerability

Risk Management

- It is not realistic to protect all systems equally.
- Risk management aims to **mitigate**, not eliminate risks.





Critical Steps for Cyber Security Incident Response Planning



IDENTIFY ASSETS & RISKS



**DEVELOP INCIDENT RESPONSE PLANS &
SUPPORT TEAMS**



EXECUTE PLAN WITH EXECUTIVE ENDORSEMENT



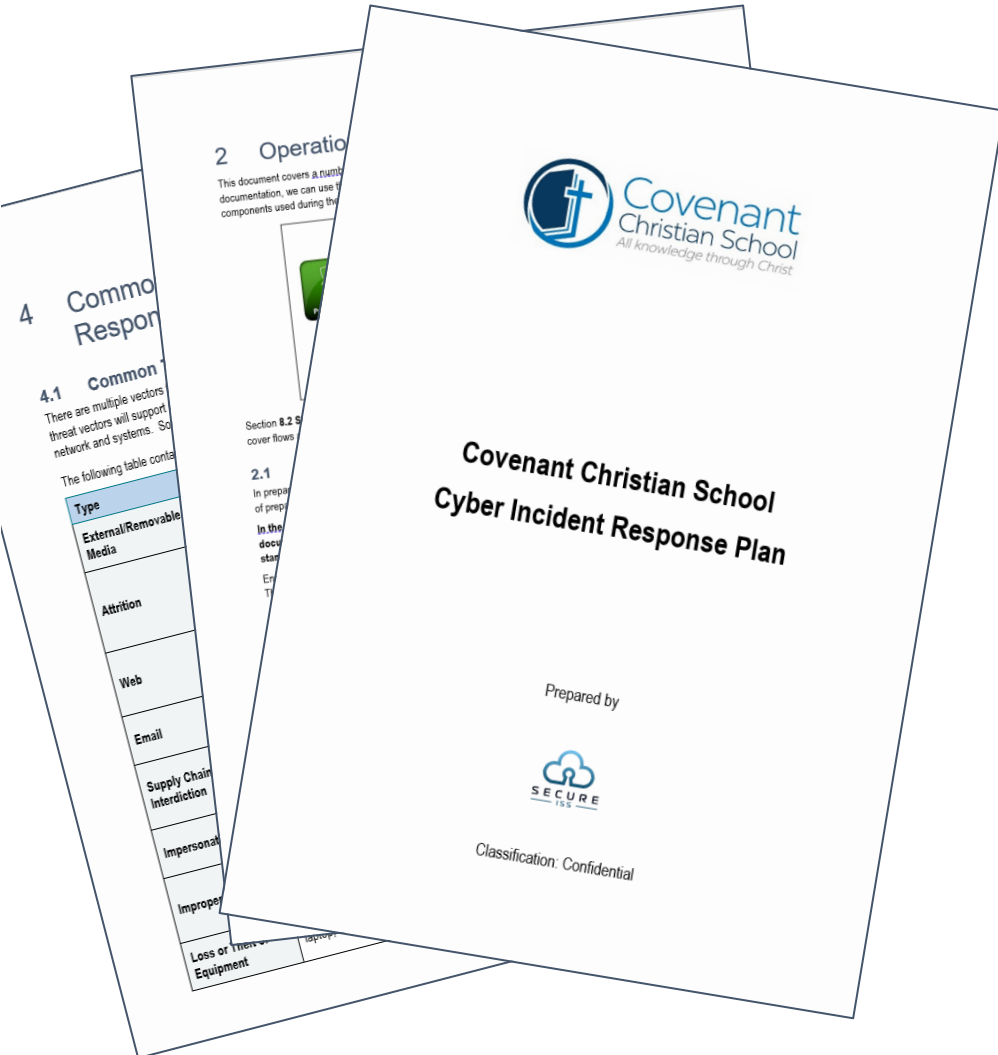
PLAN WITH YOUR PEOPLE



REASSESS & REFINE

Covenant Incident Response Plan

Table of Contents



Document control

Version history

Release approval

1 Introduction

1.1 Context

1.2 Purpose

1.3 Authority

1.4 Review

2 Operationalising this document

2.1 Preparation

2.2 Detection and Analysis

2.3 Containment, Eradication and Recovery

2.4 Post Incident Activity

3 Terminology and Definitions

3.1 What is a cyber security event?

3.2 What is a cyber security incident?

3.3 Information and Data Classification

3.3.1 Very Sensitive Data

3.3.2 Sensitive Data

3.3.3 Private Data

3.3.4 Public Data

3.3.5 Systems and Data Classification

4 Common Cyber Security Incidents and Responses

4.1 Common Threat Vectors

4.2 Common Cyber Incidents

5 Roles and Responsibilities

5.1 Points of Contact for Reporting Cyber Incidents

5.1.1 Escalation

5.2 Cyber Incident Response Team (CIRT)

5.3 Critical Incident Coordinating Team (CICT)

5.4 Board of Trustees

5.5 Third Party Vendors

5.6 Incident Notification and Reporting

5.6.1 Legal and Regulatory Requirements

5.6.2 Cyber Insurance

6 Communications

6.1 Internal Communications

6.2 External Communications

6.3 Supporting documentation

6.4 Document Storage

Identify Assets and Risks

Identify data to protect and its location, prioritise valuable assets, address vulnerabilities, conduct penetration tests, and understand financial risks.

Threat Classification Overview:

- Confidentiality
- Integrity
- Availability



Develop Incident Response Plans & Support Teams

To effectively mitigate and manage cyber security incidents.



Operational Continuity



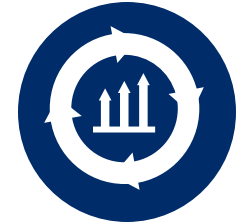
Incident Response Team Model

Operational Continuity

- Ensure essential school and business functions and processes continue
- Minimise downtime
- Avoid negative impacts
- Swift Restoration of IT Systems



Assess the School's Backup Strategy & Create a Written Backup Plan



Develop a Business Continuity Plan (BCP)

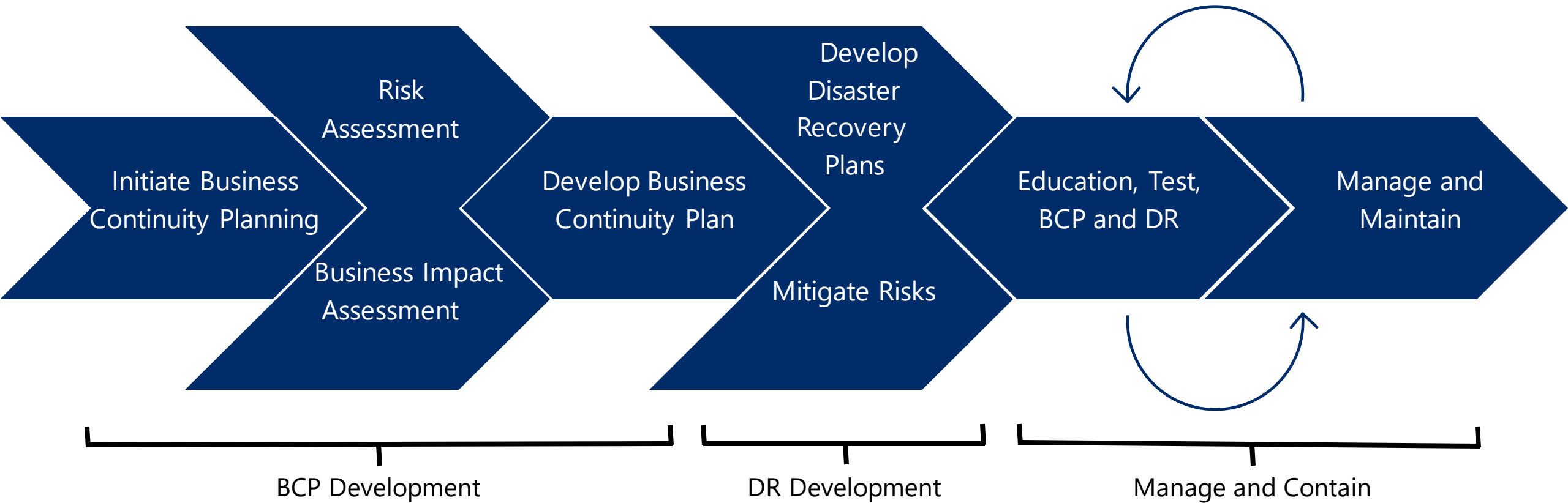


Develop Disaster Recovery Plans (DR)



Base structure on chosen Framework. i.e. CIS.

Disaster Recovery and Business Continuity



Incident Response Team Model

- Specialised team focused on rapid response to critical incidents
- Minimise damage, restore operations and protect assets
- Comprised of key stakeholders across the school
- Brings together technical, operational, and communication expertise

CIRT – **C**ritical **I**ncident **R**esponse **T**eam

CIST – **C**ritical **I**ncident **C**oordinating **T**eam

Board – School Board

Incident Response Team Model

School Board

Although not actioning response activities, Board will assist the CICT in guiding response activities particular during containment and recovery phases.

Questions that the Board should be prepared to provide guidance to:

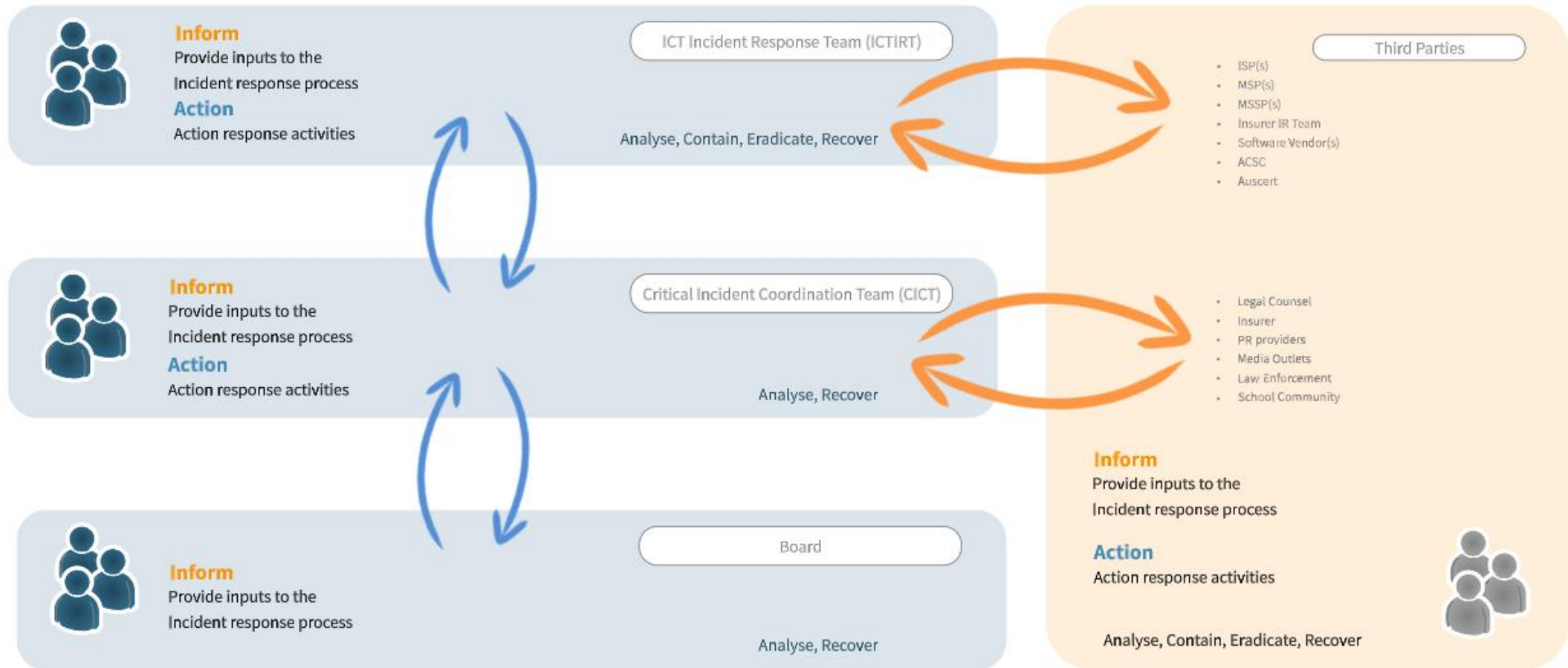
- How does the Board determine the risk appetite in relation to the reputational damage that a data breach may cause?
- How does the Board quantify the reputational damage an event may have on the school?
- In the event of a ransom demand, will the organisation consider payment?

Incident Response Team Model

Responsibility

- Incident Notification and Reporting
 - Legal and regulatory requirements
 - Cyber Insurance
- Communications
 - Internal
 - External
 - Document Storage

Incident Response Team Model



Communication with School Community in the event of an outage

Contents of Scheduled Report	2 reports which produce current Student, Parent and Staff contact details and key communication information.
Recipients of the Report	Business Manager, Director of ICT, ICT Manager (sent to roles not individuals)
Schedule and Frequency	Fortnightly
Data Transfer to Encrypted USB / Secure Storage	Work in progress
Designated Platform for Bulk Email Dissemination	SendGrid
Designated Platform for Bulk SMS Delivery	SMS Central

Execute Plan With Executive Endorsement

- Obtain endorsement and support from executive leadership
- Resource allocation for implementation
- Executive role in communication
- Escalation procedures and timely decisions
- Leadership by example
- Review and reflection

Plan With Your People

- Select people with appropriate skills for the incident response team.
- Identify groups within the school that may need to participate in incident handling, consider:
 - School Executive
 - IT Team
 - Marketing
 - Finance and Risk
 - Human Resources
 - Security and Facilities Management

Reassess and Refine

- Regularly review and update your CSIRP
- Incorporate lessons learned from previous incident
- Evolve as the threat landscape changes
- Evolve response strategies
- Team trainings and cross-department collaboration
- Conduct tabletop exercises for training, testing and refinement to ensure currency and continuous improvement.

Exercise in a Box – Table Top Exercises

<https://www.cyber.gov.au/resources-business-and-government/exercise-in-a-box>



Third Party Software Compromise - Participant Briefing

1.1 Scenario overview

This scenario investigates the risks around using third party software and the controls your organisation has in place to mitigate the impact of a third party supplier being compromised. In particular, the exercise looks at password controls, the ability to detect and respond to a compromise and the ability to cope with disruption to key services.

1.2 Objectives

The objective of this exercise is to explore how your organisation would respond to the compromise of a third party supplier. Discussions will cover the detection and response capability of your organisation, processes for dealing with service disruption, and policies in place to prevent stolen credentials being used to compromise network services. The outcomes of discussions around the events in this scenario can be an opportunity to identify areas for improvement. This exercise has the following aims:

- Understand risk associated with third party software
- Identify areas for improvement in password and authentication policy
- Clarify which network services are publically exposed
- Understand detection and response capability of organisation
- Determine processes for dealing with key services being unavailable
- Build trusted relationships and develop shared understanding between key stakeholders
- Prepare and train key staff to think about what risks they are exposed to
- Operate in a no fault environment to check and test cyber security defences and capabilities

1.3 Guidance for participants

This scenario is intended to help you understand how your organisation currently manages the risk of third party software, password policies and detection and response capabilities. Each part of this scenario is based on a realistic attack, in which your organisation's network is compromised using credentials stolen from a third party supplier. Understanding the risks associated with third party software is important. Having a strong detection and response capability, along with a password policy that encourages the



Third Party Software Compromise – Facilitator Prompts

This document should be used alongside the scenario events (injects) and discussion points which are delivered in the service. The additional questions below are to help get conversations started or explore some areas of interest in more detail. This should be reviewed before the scenario is run, and referred to throughout.

Section 1: Third Party Supplier Compromise

Facilitator guidance

The scenario starts with an online third party e-commerce tool that the organisation uses being compromised. If an e-commerce tool does not feel relevant to your organisation, the use of another online tool or cloud service that feels more appropriate can be substituted. The questions posed will still be relevant.

The compromised company has had all of their username and passwords stolen. This section aims to determine if the user has considered the risk of using third party software and if there are any policies in place to deal with a compromise.

Facilitator Prompts

1. Have you considered the benefits and risks of using third party service suppliers?
 - What are the risks to your organisation?
 - How much of your sensitive data do they have access to?
2. What processes do you have in place to respond to the compromise of a third party supplier you use?
 - What is your immediate response? Can the compromised accounts still be accessed? Should access to services be revoked?
 - Do you have a process to determine which of your services are most at risk following the compromise of a given third party? Will passwords be changed? Who will do this?
3. How can you determine which users' credentials have been stolen?
 - Do you keep accurate records of users in your organisation who have access to third party business services? Do you have a procedure to investigate where accounts on these services have been compromised?



Scribe sheet – Scenario:

Exercise Start Date:	Time:	Attendees:
Name:	Role:	
Name:	Role:	
Name:	Role:	
Name:	Role:	
Name:	Role:	
Name:	Role:	

2 | Threatened leak of sensitive data - Scribe sheet

Inject 1:

We have a number of exercises to choose from that include:



Discussion based exercises:

- A ransomware attack delivered by phishing email
- Mobile phone theft and response
- Being attacked from an unknown Wi-Fi network
- Insider threat leading to a data breach
- Third party software compromise
- Bring Your Own Device (BYOD)
- Threatened leak of sensitive data
- Supply chain risks
- Home and remote working
- Managing a vulnerability disclosure
- Supply chain software
- Supply chain ransomware attack



Micro-exercises:

- Responding to ransomware attacks
- Identifying and reporting a suspected phishing email
- Using passwords
- Connecting securely
- Securing cloud productivity suites
- Securing video conferencing services

Simulation exercises:

- A simulation exercise mimicking a cyber threat present on your organisation's network

Key Takeaways

- Operational Continuity:
 - Disaster Recovery
 - Business Continuity Plan
- Incident Response Team Model:
 - CIRT – Critical Incident Response Team
 - CIST – Critical Incident Coordinating Team
 - Responsibility: Notification, reporting and communication strategies
- Ongoing refinement, training, and reassessment

Reporting to the Board



Board Reporting Challenges

- Too much information or too little information
- Clear non-technical communication
- Articulating IT risks, vulnerabilities, and potential impacts
- Aligning IT strategy with organisational goals
- Managing cyber security and data privacy concerns

Board Reporting

Cyber Security actions based – November 2021

- Reporting was brief and dot points sufficed.
 - Cyber Security tasks were undertaken as-and-when necessary.
- Cyber Security continues to be focused on across multiple projects, including:
 - The implementation of the cloud immutable backup systems has been finalised and the daily tape backups have been retired. Weekly tape backups will continue and are held on site.
 - An external penetration tester has been selected and the testing is scheduled to run from 19 Oct - 1 Nov
 - TechServe has run a phishing campaign, which involves sending fake emails to staff, and are currently collating the results. The team received about 40 tickets and 15 walk-up queries seeking advice about the email, indicating a high level of awareness among staff.
 - Audits of passwords, licensing, and security best practice continue as part of the annual Security Uplift.

Board Reporting

Pen Test Actions based - March 2022

- Traditional dot point board report was supplemented with penetration test actions register.
- Penetration test actions were sorted by risk rating and a status column was added.

Finding ID	Risk	Title	Remediation Timeframe	Status
INPT-1	Extreme	Account and privilege management is not adequate.	3-6 Months	Open
INPT-2	Extreme	Password hygiene is not adequate.	1-2 Months	Open
ENPT-1	High	Multi-factor authentication is not required for external access to Virtual Private Network.	1-2 Months	Open
ENPT-2	High	Users are susceptible to email-based phishing attacks.	Ongoing	Open
ENPT-3	High	Website is vulnerable to web cache poisoning.	N/A	Closed
INPT-3	High	Systems are vulnerable to null session attack.	1 Month	Open
INPT-4	High	Students have local administrative privileges and wide-reaching network access on	Covenant to confirm	Open
INPT-5	High	Domain is susceptible to Kerberoasting attacks.	1-2 Months	Open
WNPT-1	High	Wireless LAN is not logically segmented from wired LAN.	3 Months	Open
WNPT-2	High	No Wireless Intrusion Prevention System (WIPS) implemented.	1 Month	Open
ENPT-4	Moderate	DNS server vulnerable to zone transfer.	N/A	Closed
ENPT-5	Moderate	Issues with certificates used to validate host identity.	3 Months	Open
ENPT-6	Moderate	DMARC has not been implemented.	1 Month	Open
ENPT-7	Moderate	DKIM has not been implemented on primary mail domain.	1 Month	Open
INPT-6	Moderate	Credentials are cached on workstations that are constantly connected to Domain Control	1-2 Months	Open
INPT-7	Moderate	KRBGT account password has not been changed for an extensive period of time.	2 Weeks	Open
INPT-8	Moderate	Directory Replication allowed to hosts other than Domain Controllers.	1-2 Months	Open
INPT-9	Moderate	Domain Administrators are not restricted to Domain Controllers.	2 Weeks	Open
INPT-10	Moderate	Administrators are assigned debug privileges.	2 Weeks	Open
INPT-11	Moderate	VMware vCenter missing critical security patches.	2 Weeks	Open
INPT-12	Moderate	Issues with certificates used to validate host identity.	1-2 Months	Open
INPT-13	Moderate	802.1X authentication not implemented on wired network.	6-12 Months	Open

Board Reporting

Enhanced Pen Test Actions based - March 2023

- Penetration test actions register was enhanced with the following additional columns.

Finding ID	Original Risk	Title	Status	Current Risk
INPT-01	Extreme	Account and privilege management is not adequate.	Complete	Low
INPT-02	Extreme	Password hygiene is not adequate.	Complete	Mitigated
ENPT-01	High	Multi-factor authentication is not required for external access to Virtual Private Network.	Complete	Mitigated
ENPT-02	High	Users are susceptible to email-based phishing attacks.	On-going	Moderate
ENPT-03	High	Website is vulnerable to web cache poisoning.	Complete	Mitigated
INPT-03	High	Systems are vulnerable to null session attack.	Complete	Mitigated
INPT-04	High	Students have local administrative privileges and wide-reaching network access on untrusted devices.	In-Progress	High
INPT-05	High	Domain is susceptible to Kerberos roasting attacks.	Complete	Low
WNPT-01	High	Wireless LAN is not logically segmented from wired LAN.	Complete	Low
WNPT-02	High	No Wireless Intrusion Prevention System (WIPS) implemented.	Complete	Mitigated
ENPT-04	Moderate	DNS server vulnerable to zone transfer.	Complete	Mitigated
ENPT-05	Moderate	Issues with certificates used to validate host identity.	Complete	Mitigated
ENPT-06	Moderate	DMARC has not been implemented.	Complete	Mitigated
ENPT-07	Moderate	DKIM has not been implemented on primary mail domain.	Complete	Mitigated
INPT-06	Moderate	Credentials are cached on workstations that are constantly connected to Domain Controller.	Complete	Mitigated
INPT-07	Moderate	KRBtgt account password has not been changed for an extensive period of time.	Complete	Mitigated
INPT-08	Moderate	Directory Replication allowed to hosts other than Domain Controllers.	Complete	Mitigated
INPT-09	Moderate	Domain Administrators are not restricted to Domain Controllers.	Complete	Mitigated
INPT-10	Moderate	Administrators are assigned debug privileges.	Complete	Mitigated
INPT-11	Moderate	VMware vCenter missing critical security patches.	Complete	Mitigated
INPT-12	Moderate	Issues with certificates used to validate host identity.	Complete	Mitigated
INPT-13	Moderate	802.1X authentication not implemented on wired network.	In-Progress	Moderate

Board Reporting for the Future

- Framework based reporting
 - Essential Eight
 - CIS Controls
 - NIST
- Cyber risk register

Cyber Risk Register Reporting

Likelihood vs Consequence = Risk Rating



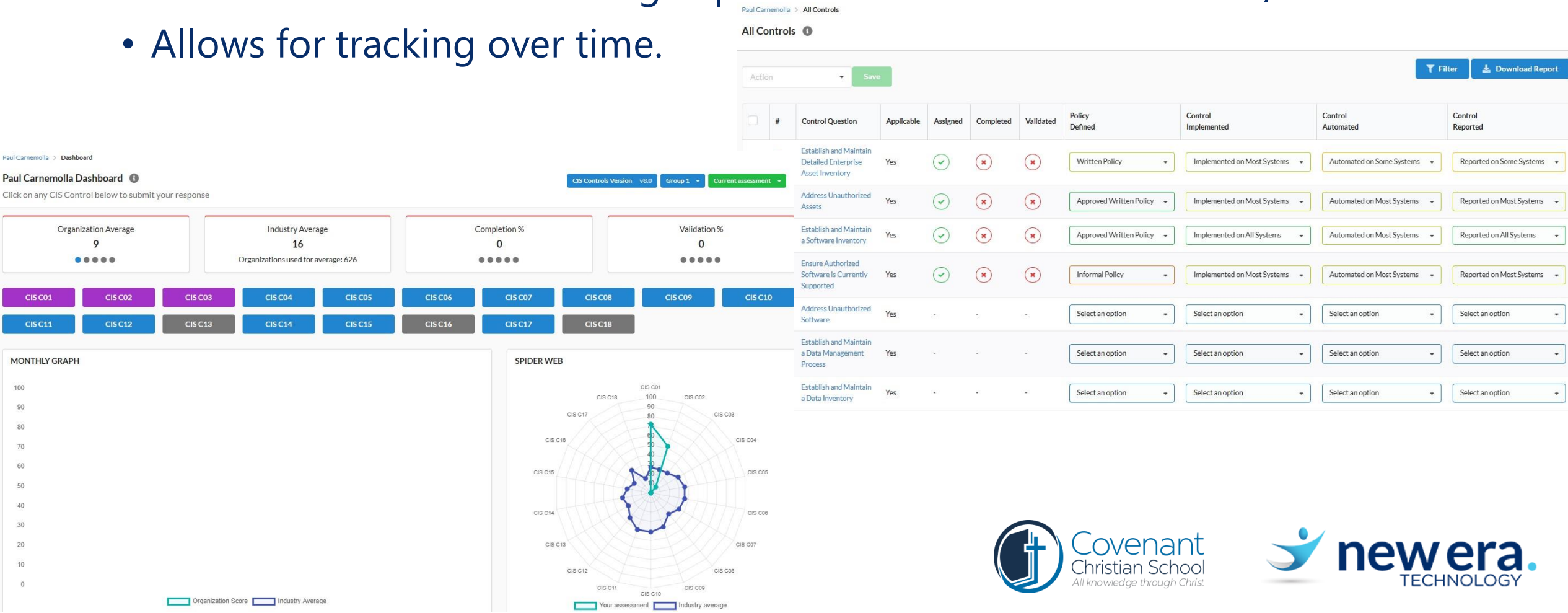
Cyber Risk Register Reporting

Risk	Cause	Likelihood	Consequence	Risk Rating	Mitigation Plan
Password compromise	Phishing email	Likely	Compromised account is lost to intruder (Moderate)	High	Implement staff training in high-risk emails
Data leak	Mixing personal and professional use of work device	Possible	Unauthorised access to data (Moderate)	Moderate	Implement strict policies and guidelines regarding personal use or business devices
Mobile data	Digital media isn't backed up	Likely	Loss of business assets (Minor)	Moderate	Compile a register of key assets and ensure routine back-up
Cloud vendor network compromise	Vendor has failed to use encrypted cloud communication	Rare	Information and assets transferred by vendor is compromised (Catastrophic)	High	Ensure vendor terms and conditions are reviewed to ensure encryption and best practice.

CIS Controls Self-Assessment Tool

<https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls>

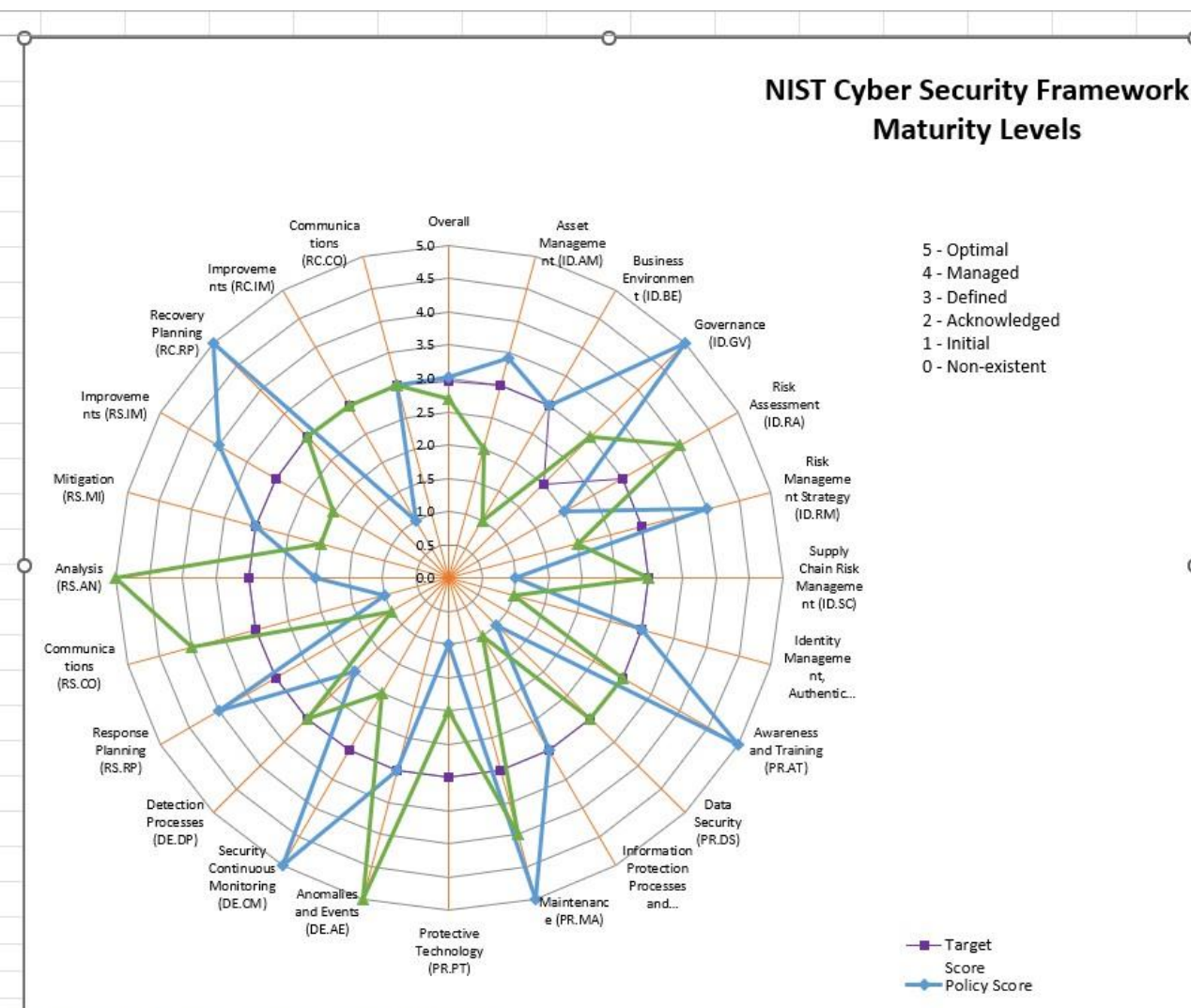
- Free online tool for assessing implementation of the CIS Security Controls.
- Allows for tracking over time.



NIST Cyber Security Framework Maturity Level

Radar Chart

NIST CSF 1.1 Categories		2022		
		Target Score	Policy Score	Practice Score
Overall		3.00	3.02	2.70
IDENTIFY (ID)	Asset Management (ID.AM)	3.00	3.42	2.00
	Business Environment (ID.BE)	3.00	3.00	1.00
	Governance (ID.GV)	3.00	5.00	3.00
	Risk Assessment (ID.RA)	3.00	2.00	4.00
	Risk Management Strategy (ID.RM)	3.00	4.00	2.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	3.00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.ID)	3.00	3.00	1.00
	Awareness and Training (PR.AT)	3.00	5.00	3.00
	Data Security (PR.DS)	3.00	1.00	3.00
	Information Protection Processes and Procedures (PR.IP)	3.00	3.00	1.00
	Maintenance (PR.MA)	3.00	5.00	4.00
	Protective Technology (PR.PT)	3.00	1.00	2.00
DETECT (DE)	Anomalies and Events (DE.AE)	3.00	3.00	5.00
	Security Continuous Monitoring (DE.CM)	3.00	5.00	2.00
	Detection Processes (DE.DP)	3.00	2.00	3.00
RESPOND (RS)	Response Planning (RS.RP)	3.00	4.00	1.00
	Communications (RS.CO)	3.00	1.00	4.00
	Analysis (RS.AN)	3.00	2.00	5.00
	Mitigation (RS.MI)	3.00	3.00	2.00
	Improvements (RS.IM)	3.00	4.00	2.00
RECOVER (RC)	Recovery Planning (RC.RP)	3.00	5.00	3.00
	Improvements (RC.IM)	3.00	1.00	3.00
	Communications (RC.CO)	3.00	3.00	3.00



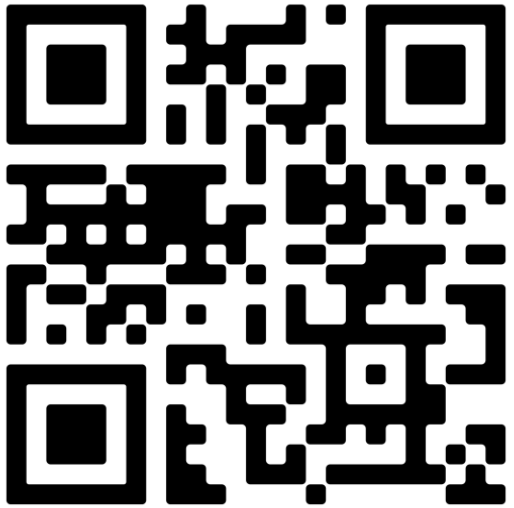
Conclusion and *next steps*



Conclusion and next steps

- Recap of key takeaways
- Importance of ongoing Cyber Security vigilance
- Encouraging collaboration and sharing best practices
- Next steps for improving Cyber Security preparedness

Today's resources
and further information



<https://www.neweratech.com/au/covenant-principals-conference-cybersecurity-in-schools/>



Contact Details

Paul Carnemolla & Solomon James



Paul Carnemolla



Solomon James

